IN THE SPECIFICATION

Please amend the specification as follows:

Please replace the last paragraph on page 9 with the following:

Figure 2(A) illustrates a function of privilege checking program 50 which automatically determines if any groups contain members who are not listed on the trusted list 54. Such groups may not warrant super user or application privilege if so assigned, as described below. The privilege checking program 50 is scheduled for periodic execution, such as monthly, based on a cron file. In step 100, the privilege checking program queries the operating system 18 for the list 54 of trusted individuals. Then, the privilege checking program queries the operating system 18 for the list 40 of all groups and the members in each group (step 102). For each group related to a specific application, the privilege checking program 50 performs steps 104-112, as follows. In step 104, the privilege checking program 50 compares the members of each group to the list 54 of trusted individuals. If all the members of the group appear in the list 54 of trusted individuals (decision 106, yes branch), then the privilege checking program 50 writes an entry in a report in a log 70 that all the members in this group are confirmed to be trusted (step 110). Referring again to decision 106, no branch, if any of the members of the group do not appear on the list of trusted individuals, then the privilege checking program 50 writes an entry in the report that all the member of the group are not confirmed to be trusted, and lists the name of the group and the names of its members who do not appear on the list 54 of trusted individuals (step 112). After steps 110 and 112, if there are more groups to check (decision 113, yes branch), the privilege checking program 50 loops back to step 104 to repeat the foregoing analysis and report for the next group.

Please replace the last paragraph on page 10 with the following:

Figures 2(B) and 2(C) illustrates another function within privilege checking program 50 which automatically determines if "application" level privilege or "super user" level privilege

has been granted to any group having a name that is generally used or specified for untrusted, user groups. This function also determines if any groups with "application" level privilege or "super user" privilege have names not generally used or specified for such higher privileged groups. In step 200, privilege checking program 50 loads from list 56 the names of groups presumed to be trusted (i.e. "super user" level privilege or "application" level privilege) and from list 58 the names of groups presumed to be untrusted (i.e. "user" level privilege). Next, privilege checking program 50 queries the operating system for the names of the application instances 12a,b,c (step 201). The operating system obtains these names from the master configuration file ~~50~~22. Next, privilege checking program 50 performs the following steps 204-216 for each application instance (because the privilege assignments can vary by application instance). Privilege checking program 50 supplies the application authority manager program 60 with the names of the groups from list 58 presumed to be untrusted such as "user", "nobody" or "staff", and asks the application authority manager program 60 for the actual privilege levels of these groups (step 204). The actual privileges levels can be "super user" privilege, "user" privilege and in operating systems which permit intermediary levels of privilege, "application" privilege or the like. The application authority manager program 60 obtains the actual privilege level for each group listed in list 58 from the respective application instance under evaluation. The application authority manager program 60 returns the actual privilege level for each such group. From the response of the application authority manager program 60, the privilege checking program checks if any of these groups actually have "super user" privilege or "application" privilege (or some other privilege higher than "user" privilege) (decision 206). If so, the privilege checking program prepares a report indicating that such group(s) has (or have) higher privilege than "user" privilege and was (or were) not expected to have higher privilege based on the name of the group (step 208). It will also include the privileges (i.e. objects for which privileges are granted) in the report for the administrator to review.